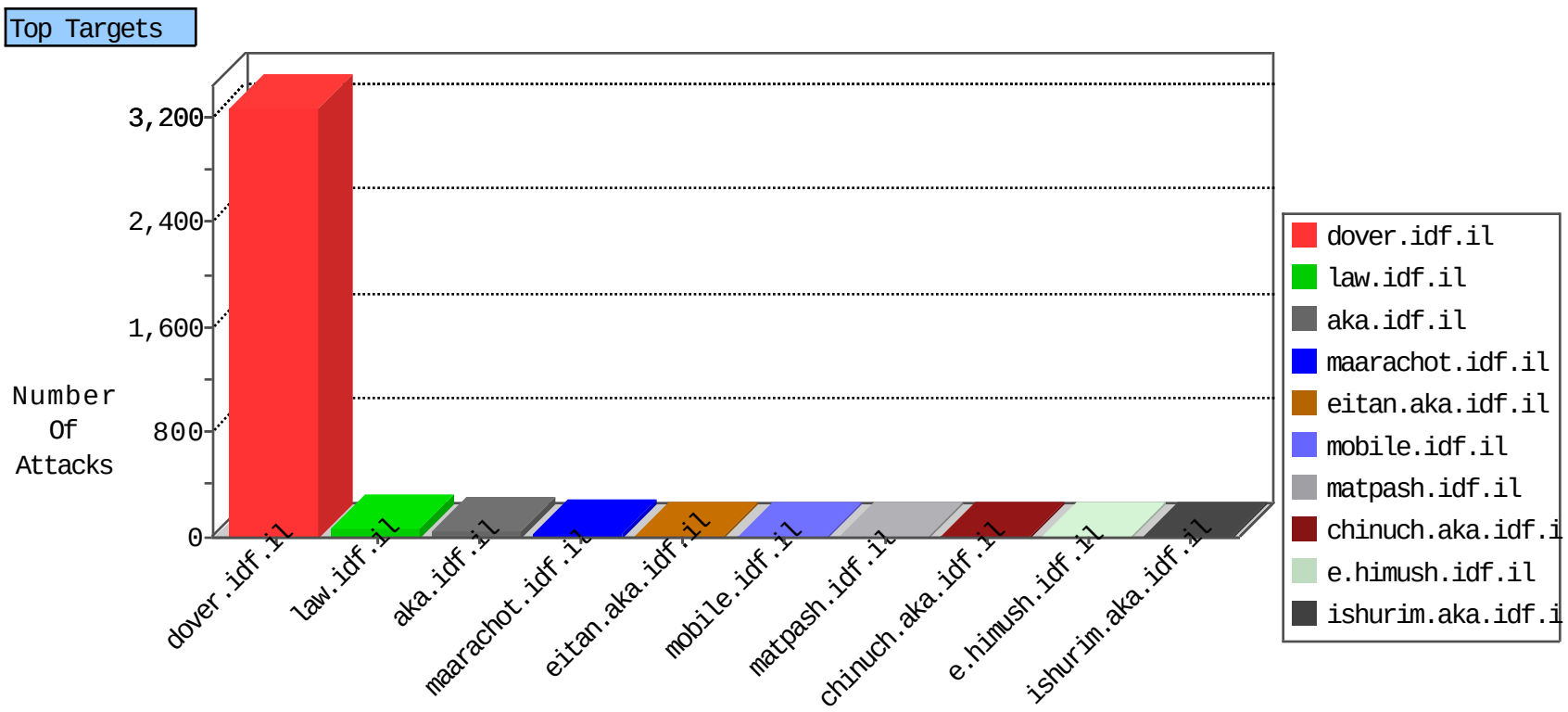
11-04-2015-02:04:05 to 11-04-2015-03:04:05

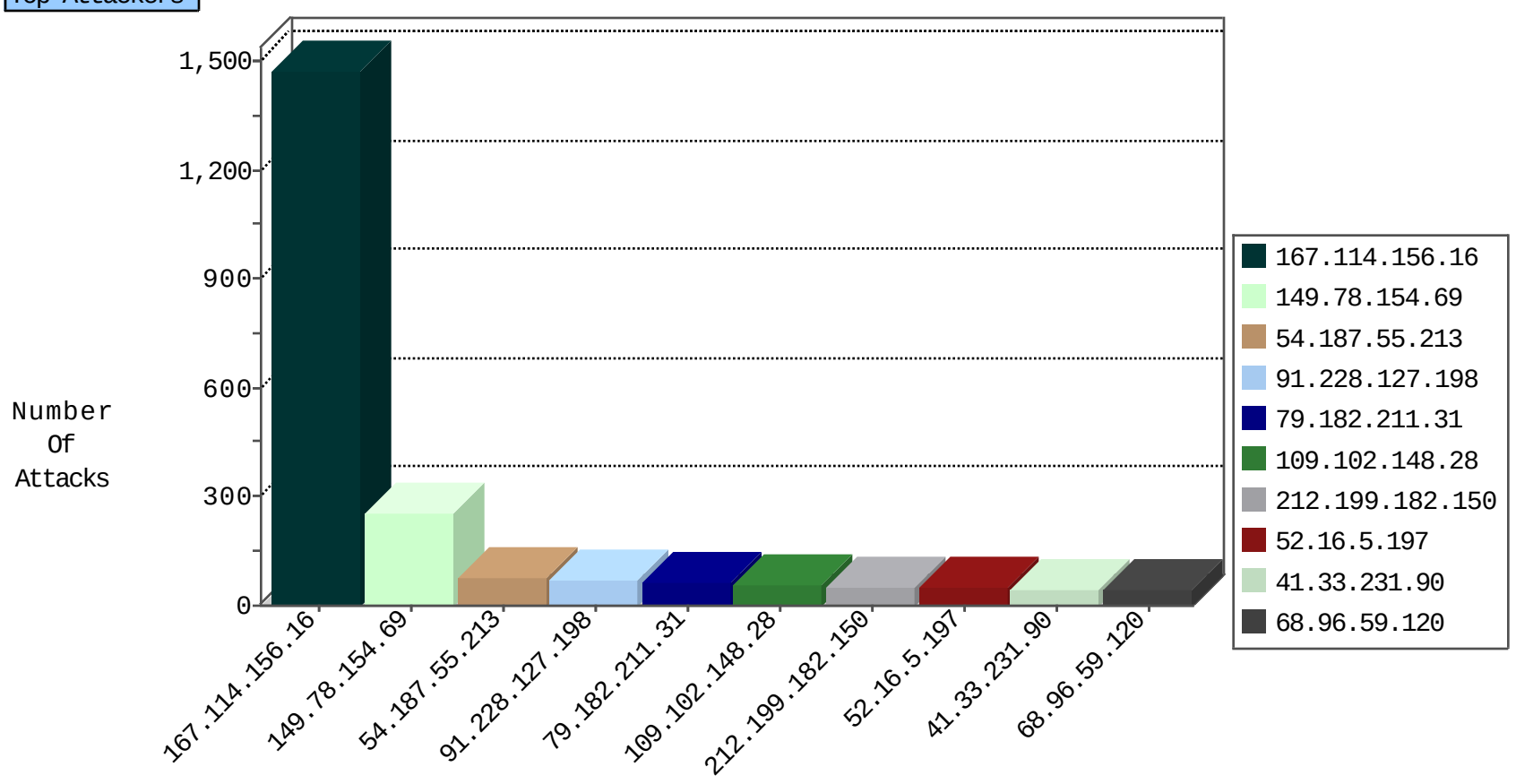
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-04-2015-02:04:05 to 11-04-2015-03:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	4167
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2442
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2067
66.249.69.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	629
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	392
68.96.59.120	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	164
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	147
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	29
66.249.67.210	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	25
50.141.109.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18
178.38.77.193	Switzerland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
81.218.235.10	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
109.102.148.28	Romania	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
85.113.118.1	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.i	Block_Udp_All_Nets	drop	3
222.186.56.42	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
85.25.103.50	Germany	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
172.98.67.23		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
85.25.103.50	Germany	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
66.249.67.250	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
71.6.186.90	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
60.48.250.166	Malaysia	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
188.138.1.218	Germany	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

11-04-2015-02:04:05 to 11-04-2015-03:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.12.204.163	Ukraine	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1

11-04-2015-02:04:05 to 11-04-2015-03:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.67.79	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
188.19.5.177	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
68.65.121.91	147.237.76.202		e.halag.idf.i	ET SCAN NMAP -sS window 1024	1

11-04-2015-02:04:05 to 11-04-2015-03:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	255
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	76
91.228.127.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
79.182.211.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	65
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
109.102.148.28	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
184.194.246.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
68.96.59.120	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
46.19.85.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
100.100.29.24		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
65.157.96.99	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
149.20.63.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.69.34	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
37.26.149.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
213.151.35.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.69.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
84.108.104.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
149.78.54.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
178.38.77.193	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.160.217.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.69.42	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.121.70.140	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
83.250.115.140	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
172.56.26.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
70.208.75.231	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
157.55.39.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.69.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.174.206.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.69.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
219.74.38.206	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
157.55.39.236	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
131.253.25.180	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
219.74.38.145	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.88.185.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
203.127.96.248	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
64.41.200.102	United States	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	7

11-04-2015-02:04:05 to 11-04-2015-03:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.201.225.11	Ukraine	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 193.201.225.11	Block	15
193.201.225.11	Ukraine	147.237.77.170	maarachot.idf.il	Multiple Admin Blocking from 193.201.225.11	Block	8
193.201.225.11	Ukraine	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	6
109.65.53.95	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.65.53.95	Block	3
109.65.53.95	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
193.201.225.11	Ukraine	147.237.77.170	maarachot.idf.il	Admin Blocking	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.77	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/kkkkkkk=d812141dkkkkkkk_d812141d	Block	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.77	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/patzar/klali/default.asp	None	1
192.151.154.130	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.74.106	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/9/112999.pdf	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
192.228.148.212	Malaysia	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to /tmunblock.cgi	Block	1
66.249.74.108	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/105495.pdf	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.173	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/2978.jpg	Block	1
192.228.148.212	Malaysia	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
66.249.79.100	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
66.249.67.79	Israel	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	1
193.201.225.11	Ukraine	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
66.249.69.15	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2349.jpg	Block	1

11-04-2015-02:04:05 to 11-04-2015-03:04:05